2026/5/20
JCA-NET セミナー
本日のテーマ

政府による暗号規制に対する闘い――何が争点になっているのか

としまる toshi@jca.apc.org

政府による通信事業者を巻き込んでの通信情報収集は世界的な趨勢にもなっています。他方で、インターネットの通信環境では、セキュリティ対策が進み、情報機関であっても以前のように簡単には通信内容を盗聴できなくなっています。その結果として、各国政府とも通信事業者に協力させて網羅的な通信情報を収集しようとする動きが活発になっています。

こうした傾向を危惧する多くのユーザーは、通信の秘密の確保の手段として強固な暗号の利用を選択しはじめています。他方で、いわゆる「民主主義」を標榜する諸国であってすら、私たちの暗号利用を規制するとともに、政府による通信の盗聴を可能にするために民間事業者の協力を強制する法制度が次々と提案されてきました。こうしたなかで、各国ともプライバシー団体や政府・企業のネット監視社会化に反対する人々による根強い抵抗運動が続いています。
今回のセミナーでは、暗号をめぐる攻防の最前線について報告し、各国で暗号規制に反対する人たちの議論を紹介します。日本もスパイ機関創設など、世界各国の政府の動向と無関係ではありません。政府や民間企業による私たちの通信情報収集に対抗する最も有力な手段である暗号について関心をもっていただく機会にしたいと思います。

目次

国家情報会議法案の問題とは

法案の概要

提案理由
⬚我が国の重要な国政の運営に資する**情報の収集調査に係る活動等**に関する重要事項を**調査審議**する機関として、内閣に国家情報会議を設置することとし、その所掌事務等に関する事項を定める必要がある。これが、この法律案を提出する理由である。

重要情報活動及び**外国情報活動**で、外国（本邦の域外にある国又は地域をいう。）の利益を図る目的で行われるものに対処するために、重要事項を調査審議する機関として、内閣に、国家情報会議を置く。

- **重要情報活動**：安全保障の確保、テロリズムの発生の防止、緊急の事態への対処その他の我が国の重要な国政の運営に資する情報の収集調査に係る活動
- **外国情報活動**： 公になっていない情報のうちその漏えいが重要国政運営に支障を与えるおそれがあるものを取得するための活動、及びこれと一体として行われる不正な活動

国家情報局は、内閣官房に置かれ、その役割は、
- 重要情報活動及び外国情報活動への対処
- 特定秘密の保護に関する法律（平成二十五年法律第百八号）第三条第一項の特定秘密の保護に関するもの

政府による事前の情報収集活動が必須

私達は、これまでの戦前戦後を通じて政府による法律の恣意的な解釈が政府への批判的な言論活動や社会運動の弾圧に利用されてきた歴史を忘れてはならない。こうした歴史的な文脈を踏まえて、法案の条文の意味するところを解釈する必要がある。国家情報局が対象とする事柄は「重要情報活動及び外国情報活動への対処であって、外国の利益を図る目的で行われるもの」という場合、政府がどのようにしてある活動が「外国の利益を図る目的で行われるもの」であると判断できるのだろうか。

つまり、

– 人々の活動が「重要情報活動」であるかどうかを判断するためには、**政府は、活動の実態を把握するための調査活動を行うことが前提**になる。

– 「重要情報活動」の定義は「安全保障の確保、テロリズムの発生の防止、緊急の事態への対処その他」と幅広く、対象を恣意的に拡大できるために、社会運動など**ほとんど全ての人々の活動が対象**になりうる。これまでも警察は日常的にテロ対策を掲げた警備体制を敷いていること、緊急事態については軍事から災害まで幅広いこと、安全保障も狭義の軍事安全保障だけでなく経済安全保障や人間の安全保障なども含意され、医療、福祉や社会保障分野も含まれる。

社会運動や市民運動が「重要情報活動」とみなされる可能性

社会運動にとって、政府情報を収集する活動は重要な活動の一環である。こうした活動が「重要情報活動」とみなされる可能性がある。たとえば、

- 米軍基地や自衛隊基地を監視する運動
- 反原発運動。原発施設がテロ対策の重点施設とされていることから、その活動が「重要情報活動」とみなされる可能性がある。
- 地域開発に反対する運動。政府が重要インフラに指定している産業は日本の基幹産業を網羅しており、こうした分野に含まれる企業活動に対する抗議運動などが重要情報活動とみなされる可能性がある。
- 日本で暮す外国籍の人達も、その国籍や出身国によっては政府の監視対象として通信情報などを把握されることにもなりかねない。言うまでもなく、こうした人達を支援する活動も監視対象になりうる。

上に挙げたケースは、例示にすぎず、対象範囲はほぼすべての経済活動分野、政治活動分野をカバーするものになる。

ジャーナリストや市民メディアの情報収集への圧力

ジャーナリストも監視対象になる。「重要情報活動」とは「我が国の重要な国政の運営に資する情報の収集調査に係る活動」と定義されおり、公開情報の収集も含まれる。そもそも国政運営に資する情報は、多くの人々にとってみずからの利害にも関わり、関心をもつべき情報であってジャーナリズムがこのような情報を収集することは必須の事柄である。こうした取材活動が取り締まりの対象となる「情報収集活動」であると解釈される可能性があり、特に外国のメディアやジャーナリスト、フリーランサーや市民メディアが標的にされかねない。こうした疑いをかけられることを畏れてメディアが取材活動や報道を規制・自粛する可能性がある。

このことは、一般市民によるネットでの情報発信についてもあてはまる。世界的にみて、多くの市民メディアや調査報道機関は、政府の犯罪や腐敗の告発において、いわゆるオープンソースによる調査で大きな成果をあげているために、政府はこうした調査報道を規制したがっているかもしれない。
他方で政府への批判的な投稿に対して、政府支持のインフルエンサーやブロガーなどから「重要情報活動」だというレッテルを貼られて、脅迫的なキャンペーンが展開されることもありえる。

外国の利益を図る目的の活動かどうかをどうやって判断するのか？

法案では、外国とは「本邦の域外にある国又は地域」と定義されているだけだ。この「外国」というあいまいな文言は「外国政府」とも「外国籍の人」ともとれる。日本が敵対国とみなす国の政府だけでなく、その国の出身者の正当な情報収集活動が監視対象にされる可能性がある。
「外国＝敵」とみなし、広範囲に収集された「重要情報活動」から、**「外国の利益を図る目的**で行われるもの」を抽出・監視することが正当化される、という場合、政府が「外国の利益を図る目的の活動」であると判断するには、当該の人や団体と外国との繋りを把握することが必要になる。
「外国の利益」の範囲は広く、いわゆる「産業スパイ活動」が含まれる可能性がある。この場合、企業で働く外国籍の人々に対して**産業スパイではないことを証明できるような仕組みが必要**になり、これがいわゆる経済安保で議論となったセキュリティ・クリアランス制度と連動し、外国籍の人達にはより厳しいチェックが課されることが想定できる。

法案は**外国の利益＝日本の不利益という敵対的な発想**から外国の利益になる情報活動を敵視している。これは正しくない。特に、市民や民間レベルでの国境を越えた情報活動では、国益に反しても双方の人々にとっての利益になる情報収集活動がありえる。「外国の利益」条項は差別条項であり認められない。

外国の利益を図る目的での情報収集は違法なのか？

そもそも「外国の利益を図る目的」での情報収集を監視対象とすることが、日本の法体系において許されているのだろうか。公開情報の収集であってもその意図如何によって犯罪監視できるとすれば、この意図の解釈が政府や国家情報局による独断に基くことになりかねない。同時に、この「外国＝敵」規定は米国のような「同盟国」には適用されないだろう。日本の米軍基地が諜報活動を行なっていることはスノーデンの告白でも明かになっているが、こうした米軍や米国の諜報機関の日本国内での活動を政府は取締られていない。むしろ米国と日本の情報機関が連携して、日本国内で収集可能な「敵国」の情報収集にあたる可能性の方が高い。

憲法上、外国の利益を図る目的での言論表現活動は禁じられていない。にもかかわらず、日本国内で「外国」に利するような言論活動を行なうことが摘発や監視の対象にされたり、当該国出身者であるというだけで、当該国政府と同一視されて、その正当な情報収集活動を監視対象にするのは憲法違反である。更に、インターネットのグローバルな情報通信環境を前提にした場合、外国の利益を図る目的で海外から日本国内にアクセスし情報収集する行為もまた監視対象になり、場合によってはこうしたアクセスを規制・遮断するなどの措置がとられれば多様な情報の流通そのものが阻害される。

「重要情報活動」への対処の前提としての網羅的な情報収集体制構築

このように「重要情報活動」への対処とは

- まず最初に、できるだけ広範囲にわたって通信情報を収集する
- この収集データから「重要情報活動」を絞り込む
- 「重要情報活動」に該当する個人や団体の活動実態を把握する
- この実態把握の段階で、たとえば、通信情報、時には通信の内容が把握される
- 外国の利益を図る目的と判断されれば監視・摘発対象になる。
- そうではない情報であっても廃棄されずにデータとして保管されビッグデータの一部として将来の活用が図られる。

結果として、広範囲に多くの人々や団体の動静を把握し、収集された情報を蓄積する体制が構築される。

現代では、あらゆる人々がネットの情報発信主体として、様々な情報収集活動を展開している。「重要情報活動」なのかどうかの判断には、人々の情報を網羅的に収集してその内容を分析することが必須になる。そして除外されたデータであっても、それを保存することは禁じられていない。今現在は「重要情報活動」に属さないデータであっても、それが5 年後、10 年後には「重要情報活動」としての意味をもつことはありうるので、収集したデータを政府は最大限蓄積する体制をとるだろう。

（参考）国家情報会議設置法案（抜粋）

（趣旨）
第一条　この法律は、国家情報会議の設置及び所掌事務等について定めるものとする。
　（設置）
第二条　重要情報活動（安全保障の確保、テロリズムの発生の防止、緊急の事態への対処その他の我が国の重要な国政の運営（以下この条において「重要国政運営」という。）に資する情報の収集調査に係る活動をいう。次条及び第七条において同じ。）及び外国情報活動への対処（公になっていない情報のうちその漏えいが重要国政運営に支障を与えるおそれがあるものを取得するための活動（これと一体として行われる不正な活動を含む。）であって、外国（本邦の域外にある国又は地域をいう。）の利益を図る目的で行われるものへの対処をいう。次条及び第七条において同じ。）に関する重要事項を調査審議する機関として、内閣に、国家情報会議（以下「会議」という。）を置く。
　（所掌事務）
第三条　会議は、次の事項について、調査審議する。
　一　次に掲げる事項その他の重要情報活動に関する基本的な方針
　　イ　関係行政機関における重要情報活動の重点
　　ロ　関係行政機関の連携及び協力に関する重要事項
　　ハ　情報収集衛星（我が国の安全の確保、大規模災害への対応その他の内閣の重要政策に関する画像情報の収集を目的とする人工衛星をいう。）の開発及び運用に関する重要事項
　二　外国情報活動への対処に関する基本的な方針
　三　重要情報活動の推進及び外国情報活動への対処に際し配慮すべき内外の情勢についての基本的な認識及び評価
　四　重要情報活動の対象となる事案のうち特に重要なもの又は外国情報活動への対処に係る特に重要な事案の総合的な分析及び評価
　五　その他重要情報活動又は外国情報活動への対処に関する重要事項
（事務）

第十二条　会議に関する事務は、国家情報局において処理する。

（参考）特定秘密の保護に関する法律第三条第一項（抜粋）と内閣法

秘密保護法

（特定秘密の指定）

第三条　行政機関の長．．．は、当該行政機関の所掌事務に係る別表に掲げる事項に関する情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるもの（日米相互防衛援助協定等に伴う秘密保護法（昭和二十九年法律第百六十六号）第一条第三項に規定する特別防衛秘密に該当するものを除く。）を特定秘密として指定するものとする。

内閣法

第十六条の二　内閣官房に、国家情報局を置く。

　２　国家情報局は、次に掲げる事務をつかさどる。

　　一　第十二条第二項第二号から第五号までに掲げる事務のうち、国家情報会議設置法（令和八年法律第▼▼▼号）第二条に規定する重要情報活動及び外国情報活動への対処並びに特定秘密の保護に関する法律（平成二十五年法律第百八号）第三条第一項の特定秘密の保護に関するもの（内閣広報官の所掌に属するものを除く。）

　　二　第十二条第二項第六号に掲げる事務

　　三　国家情報会議設置法第十二条の規定により国家情報局が処理することとされた国家情報会議の事務

　　四　国家情報会議設置法第七条の規定により国家情報会議に提供された資料又は情報その他の前三号に掲げる事務に係る資料又は情報を総合して整理する事務

個人情報保護法例外規定

今国会には国家情報会議法案だけでなく個人情報保護法の改悪案も提出されている。この二つの法案の関係は？

今国会に提出されている個人情報保護法改正案では「個人データ等の第三者提供及び公開されている要配慮個人情報の取得について、統計情報等の作成にのみ利用される場合は**本人同意を不要とする**」とか「取得の状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかな取扱いである場合は**本人同意を不要とする**」というように本人同意を緩める条文が設定されている。

この改正案と国家情報会議 / 局の役割とを一体のものとして理解する必要がある。

すでに個人情報保護法のガイドラインには「例外的に利用目的以外の目的のための利用及び提供が認められる場合」として以下の文言がある。

「５‐５‐２　例外的に利用目的以外の目的のための利用及び提供が認められる場合」：「**法令の定める場合、**又は人の生命、身体若しくは財産の保護のために必要がある場合その他公的な利益のために個人情報を利用又は提供することがやむを得ないと認められる場合には、利用目的以外の利用及び提供が許され得る。」

個人情報保護法例外規定（2）

国家安全保障を前面に押し出している国家情報会議＝国家情報局による情報収集活動が「**法令に定める場合**」になれば、目的外利用の歯止めがなくなり、個人情報保護法は骨抜きになる。
また、このガイドラインで「人の生命、身体若しくは財産の保護」と述べられている箇所は、国家安全保障に限定されていない。したがって医療情報を官民連携で共有するなど営利目的での情報提供も、医療である以上生命、身体の保護に関わるという屁理屈で許容されかねない。

個人情報保護法改正案は個人情報の共有や提供の例外を広げる方向にあり、この改正が国家情報会議による個人情報の収集のハードルを下げることになる。一見すると相互に関係のない立法事実を掲げているが、根底ではひとつに繋がっている。
つまり、より広範に、より容易に個人情報を国策に利用する、ということだ。しかもインターネットのグローバルな環境においては、熾烈な個人情報の資源獲得競争が展開されており、個人情報の官民利活用を軍事とビジネス両面で、国境を越えた国外での情報収集にまで広げる思惑があるとみてよいだろう。

第１章　重要電子計算機に対する特定不正行為による被害の防止に関する基本的な事項

第１節　本法による各種措置を行うこととなった背景・経緯

サイバー脅威は国民生活・経済活動を脅かす**まさに災害のような存在**

- ○ 昨今、国家を背景としたサイバー攻撃が行われるなどサイバー分野における安全保障の確保が切迫した課題に。
- ○ 攻撃の巧妙化・高度化が進み、サイバー攻撃関連通信数も増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大。
- ○ あらゆる主体がサイバー攻撃のリスクに晒され、一主体に対する攻撃による被害の影響が社会全体にまで波及するおそれ。

⇒「**国家安全保障戦略**」（令和４年12月国家安全保障会議及び閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させることとした。これに基づき、**サイバー安全保障分野での対応能力の向上に向けた有識者会議**が開催され、令和６年11月に提言を取りまとめ。

⇒ 令和７年２月、当該提言に基づく法律案が国会に提出され、国会での審議を経て、①**官民連携の強化**及び**通信情報の利用**に係る制度の導入を内容とする**サイバー対処能力強化法**、及び②アクセス・無害化措置に係る制度の導入等を内容とする同整備法が成立し、同年５月23日に公布。

○ 法の段階的な施行を経て、基本方針に基づき効果的かつ適正に制度の運用を図ることを通じ、**関係機関・関係者が一体となってサイバー脅威に対する我が国のサイバー対処能力を強化**する必要。

サイバー対処能力強化法

第２節　制度の基本的な考え方

法に基づく各般の施策を実施することにより、以下①～③の機能を**抜本的に強化**

① 情報の収集

通信情報の利用

（ア）当事者協定
（イ）同意によらず通信情報を利用する措置（外外通信目的送信措置等）

官民連携の強化

（ウ）特定重要電子計算機の届出義務
（エ）特定侵害事象等の報告義務
（オ）協議会の枠組

② 情報の整理・分析

- (ア)～(オ)の制度に基づき収集した情報
- その他の手法により取得した情報

↓ 整理・分析（情報のデータベース化、照合等）

次の情報をそれぞれ作成：
- 総合整理分析情報
- 提供用総合整理分析情報
- 周知等用総合整理分析情報

③ 情報の提供

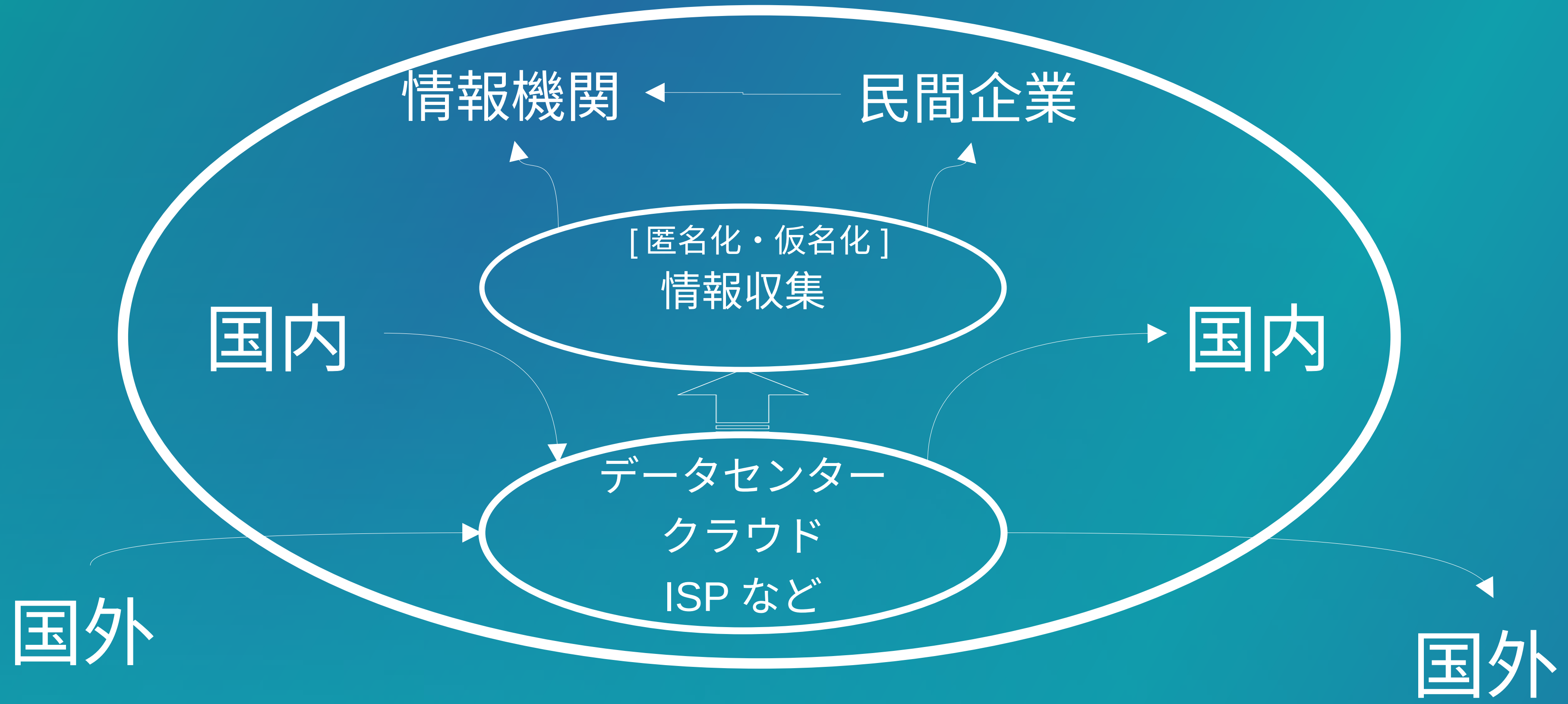
作成した総合整理分析情報等を被害防止等に役立てるため、次の者に適切に提供

- 行政機関等
- 外国の政府等
- 協議会の構成員
- 特別社会基盤事業者
- 電子計算機を使用する者
- 電子計算機等供給者

法に基づく上記の各施策について、以下を**施策の駆動力の両輪**として制度運用を図る。

全てのステークホルダーがメリットを

サイバー対処能力強化法に基づく基本方針の概要　2025/12
内閣府政策統括官（サイバー安全保障担当）　https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin_gaiyou.pdf



- 国内にデータセンターなどを設置することで国外のデータを国内に呼び込む
- 個人情報保護法の例外規定や匿名化・仮名化を利用して官民でのデータ利活用
- ビッグデータや AI を活用して匿名データの実名化

⇒ 暗号化はこの目論見を破綻させるかも

技術的な対抗手段＝暗号化をめぐる熾烈な闘い

ビッグデータの収集が世界規模で展開され、各国で、また企業間でデータの争奪戦が加熱しており、日本政府もまた、官民連携によるデータ利活用に積極的に乗り出している。政府の思惑は二つある。
- 国家安全保障（戦争）を念頭にサイバー領域の網羅的なデータ収集体制の構築
- 日本企業の国際競争力強化をねらって、国内外のデータ収集支援体制の構築

この観点からみたとき、国家情報会議／局をめぐる動きと、民間のデータ利活用を促進するための個人情報規制の緩和をめざす個人情報保護法の動向は、個人データの網羅的な収集とその利活用の推進という観点では利害が一致する。

ビジネスであれ軍事・治安であれ個人データの収集が焦点になっているという場合、これに対抗できる手段として、法制度による規制に期待したいところだが、政権与党も野党もプライバシーや人権を最優先にした法制度には後ろ向きだ。これはどこの国にも共通してみられるもので、法による規制の限界になっている。これに対して、各国の人権団体やプライバシーを重視する民間企業などは、暗号化によるデータ防御に積極的に取り組んでいる。暗号技術の高度化もあり、量子暗号のように、容易に解読できない暗号の実用化も進んでいる。

技術的な対抗手段＝暗号化をめぐる熾烈な闘い（2）

しかし現実には、暗号化が通信を全面的に覆うようにはなっておらず、インターネットの通信経路上で https やスマートフォンのデータの暗号化が普及している反面、プロバイダーのサーバーやクラウドでのデータの暗号化は進んでいないし、エンドユーザーが使用しているパソコンのデータの暗号化も進んでいない。エンド・ツー・エンド暗号化のように自分と相手双方のみしかデータを読めず、その中間にあるさまざまなサービスやネットワークが完全に暗号化されるケースはまだ一般的ではない。とはいえ、年々暗号化サービスの利用は広がりをみせており、**網羅的な情報収集を目論む政府にとっては、収集データが暗号化されて解読不能という自体が増加していることに危惧を持っている。**

これに対して政府側が対抗措置として

- 暗号化サービスの利用それ自体を禁止
- 政府が解読可能な暗号化サービスのみを適法とする
- ユーザーのパソコンやスマホで暗号化される前のデータを収集する

など様々な方策が試みられてきている。各国政府は、立法化が可能な世論形成を意図して、たとえば、子どもの性的搾取対策とかテロ対策など、人権団体など世論が反対しづらい課題を前面に押し出した暗号規制導入の動きが各国でみられる。いったん規制が導入されれば、当初の目的を逸脱し様々な分野で暗号規制がほどこされ、私たちのコミュニケーションの権利が脆弱になる。

そもそも暗号化の何が争点になっているのか

政府の言い分：暗号化は政府による通信情報の網羅的な収集＝監視能力を弱体化させる

ネットのコミュニケーションでは、以下の箇所が暗号化されないままのデータとなる

- 人がパソコンやスマホに入力する際に、パソコンやスマホの画面に入力データが表示される場合
- プロバイダーのサーバー、クラウドやユーザーのデバイスにデータが暗号化されずに保管される場合

暗号化されるのは

- 通信回線上で https で接続されている場合
- プロバイダーのサーバー、クラウドで暗号化されてデータが保管される場合
- エンド・ツー・エンド暗号化が用いられている場合



政府の言い分とは

01 犯罪者は証拠を隠滅するための暗号を利用している。

02 裁判所の令状で押収したデータが暗号化されていて解読できない場合、令状の効力が発揮できないことになる。

03 裁判所の令状の趣旨は、暗号化される前の元データを押収することにある。

04 暗号サービス事業者は捜査機関が暗号解読できるようにする義務がある。

05 捜査機関が解読できない暗号サービスは利用できないようにすべきだ。

日本政府「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」

日本政府は、 2020 年 10 月 11 日に発出された「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」（以下「ステートメント」と呼ぶ）に、英国、米国、オーストラリア、ニュージーランド、カナダ、インドとともに署名

日本語訳 https://jca.apc.org/jca-net の取り組み / 暗号規制に反対します―日本政府は「エンドツー /

2020 年 10 月 11 日

- 暗号化技術の実装は、性的に搾取された子どものような社会の非常に脆弱なメンバーを含め、公共の安全に重大な課題をもたらす。
- 暗号化がコンテンツへのいかなる法的アクセスも完全に排除する方法で適用される場合についての我々の深刻な懸念に対処するよう業界に強く要求
- 合理的で、技術的に実現可能な解決策でテクノロジー企業が政府と協力

日本政府の共同声明の内容

テクノロジー企業に対して

01 **犯罪捜査や起訴を容易**にすること。

02 **法執行機関が解読、利用することができる形式**でコンテンツにアクセスできるようにすること。

03 政府が設計決定に実質的かつ真に影響を与える方法で**法的アクセス**を促進する。

日本政府の共同声明の内容

エンドツーエンドの暗号化のリスク

01 利用規約違反を特定して対応する企業自身の能力を著しく損なう。

02 法執行機関がコンテンツにアクセスすることができなくなる。

「暗号化は不可欠であり、プライバシーとサイバーセキュリティは保護されなければならないが、このことによって、法執行機関やテクノロジー業界自体が、オンライン上の最も深刻な違法コンテンツや活動に対して全く対処できないという代償を伴うべきではない。」

日本政府の共同声明の内容

要求項目

01 このコミットメントは、**デバイス暗号化、カスタム暗号化アプリケーション、統合プラットフォーム全体の暗号化など、利用可能な暗号化サービスの範囲にも適用**される

02 我々は、**プライバシーやサイバーセキュリティを犠牲にすることなく公共の安全を保護すること**はできないという主張に異議を唱える。

03 我々は、これらの重要な価値観それぞれを保護するアプローチが可能であると強く信じており、**産業界と協力して、相互に合意可能な解決策**について協力するよう努力している。

JCA-NET
声明

2021年3月

(JCA-NET声明)暗号規制に反対します―日本政府は「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」から撤退を!!

反対の理由とは

01 憲法21条で定められた「通信の秘密」条項に明確に違反

02 法執行機関などが読取・利用できるように暗号化を弱体化

03 **「脆弱な人びと」をより脆弱にしてしまう**

04 法執行機関が私たちの通信の秘密に対して**特権的な権限を行使できるような通信インフラを構築**し、監視国家化を促す

https://jca.apc.org/jca-netの取り組み/暗号規制に反対します―日本政府は「エンドツー/

「『脆弱な人びと』をより脆弱にしてしまう」とはどのようなことか？

たとえば、本国の政府からの迫害を逃れて、海外から難民などとして日本に避難してきた人達は、本国政府の監視や弾圧の標的になる。日本政府と当該国の政府が友好関係にある場合、両方の政府から監視や弾圧の対象になりうる。
このような人達が、監視や迫害を恐れることなく、自由に通信を行うためには、通信内容を把握されない手段をとることが必要になる。このためには、政府によって解読できない暗号技術の利用が必須になる。
特にこうした当事者を支援する人権団体や弁護士との連絡に暗号化は欠かせない。

「法執行機関が私たちの通信の秘密に対して特権的な権限を行使できるような通信インフラを構築し、監視国家化を促す」とはどのようなことか？

インターネットの安全性を向上させるために、インターネット上のデータは暗号化される場合が多くなっている。しかし、プロバイダーのサーバーではまだ暗号化されないままでデータが保管されている場合があったり、プロバイダーの協力があれば、サーバーの暗号化されたデータを解読(復号)可能な場合がある。政府は、プロバイダーなどに暗号解読を義務づけようとする傾向がみられる。

（カナダ）法案 C-22（合法的アクセスに関する法律）

「情報への適法なアクセスを支援する法律」は、サービス事業者に対し、通信や機密データにアクセスする「技術的手段」の導入を強制。

グローバル暗号化連合：（カナダ）法案 C-22（合法的アクセスに関する法律）に関する公開書簡

「強力な暗号化は、個人情報を悪意ある者の手に渡らないようにするために不可欠です。個人を特定可能な機密データをオンラインサービスが収集、集約、販売することが増え続けているデジタル社会において、暗号化はオンライン上のプライバシーとセキュリティを守るための最後の砦となることが多々あります。人々や企業が利用可能な最強のセキュリティツールで自らを守ることを妨げることは、悲惨な結果を招くでしょう。」

法案の影響とは

01 カナダの人々とカナダの機関を、外国による監視や干渉にさらすことになる。

02 カナダ国内および海外の人々、特に子どもや社会的に脆弱なコミュニティのセキュリティとプライバシーを危険にさらす。

03 カナダのデジタル経済の成長と回復力を損なう。

04 カナダの人々に、サイバー犯罪によるコスト増の負担を強いることになる。

法案の影響とは

暗号化されたデータや通信へのバックドアアクセスを提供することは、何百万人もの遵法市民のプライバシーとセキュリティを侵害することなしには不可能

プライバシーとセキュリティへの悪影響とは

新しい AI システムの登場

- ソフトウェアを自律的にスキャン⇒暗号化にほどこされたバックドアによって生じた脆弱性を発見⇒侵入するための攻撃コードを生成
- AI によって、脆弱性の発見から悪用までの時間が数ヶ月からわずか数時間に短縮され、義務付けられたバックドアは敵対者によってほぼ瞬時に武器化される

法案の影響とは

参考（東京新聞）政府、米最新ＡＩの使用権要求⬚サイバー攻撃悪用に懸念

「米新興企業アンソロピックの最新人工知能（ＡＩ）「クロード・ミュトス」を巡り、日本政府が使用できるようアクセス権の提供を求めて交渉していることが１２日、分かった。最新ＡＩを悪用したサイバー攻撃の懸念が拡大しており、対策につなげる狙い。近くアンソロピックと政府関係者が協議する方向だ。 ⬚クロード・ミュトスは、インターネット上の脆弱性を見つけ出す能力が飛躍的に向上したとされる。アクセス権を持つのは米グーグルなどのＩＴ企業や金融機関に限られており、国や公的機関が提供を要望する動きが出ている。 ⬚日本政府はミュトスを活用できる環境を整え、提供を求めていく考えだ。アクセス権を取得できれば、ＡＩ開発に関連した知見やノウハウを得ることも可能になる。中国やロシアからのサイバー攻撃に対抗したい狙いもあるとみられる。 ⬚ミュトスを悪用すれば、幅広い分野のシステムの混乱を招くようなサイバー攻撃もできるとされる。高性能なＡＩは今後も次々と開発される可能性があり、政府としてアクセス権を獲得していくことが国益になると判断した。」

https://www.tokyo-np.co.jp/article/487452

セキュリティ脆弱性を見つける新AI、高性能すぎて公開見送り --「悪用を懸念」とAnthropic

https://japan.cnet.com/article/35246255/

Anthropicの「Claude Mythos」が示す、自律的サイバー攻撃の新たな脅威

https://forbesjapan.com/articles/detail/96654

EUのチャット・コントロール

- 2022年　欧州委員会は、オンライン上での子どもの性的虐待の拡散や、オンライン上での子どものグルーミングを阻止することを目的とした法律を提案(修正案など何度か提起されて現在に到る)
- そのために、この法案では、当局はアプリやその他のオンラインサービスのプロバイダーに対し、ユーザーのメッセージ、写真、電子メール、ボイスメール、その他の活動をスキャンするよう強制する。
- エンド・ツー・エンドで暗号化されたアプリの場合、このスキャンはユーザーのデバイス上で行う。

経緯

2022

「チャット・コントロール」の初期提案

欧州委員会は、すべての電子メールおよびメッセンジャープロバイダーに対し、児童性的虐待素材の有無を通信内容からスキャンすることを義務付ける、当初の「チャット・コントロール」提案を公表した。

https://fightchatcontrol.eu/#overview

2025/7/1

デンマークの議長国就任
デンマークが EU 理事会議長国を引き継ぎ、就任初日に「チャット・コントロール」を最優先の立法課題として再提示した。合意が得られれば、 2025 年 10 月 14 日の採択を目指している。

2025/7/28

機運高まる： 15 カ国がチャット・コントロール支持
EU 加盟国 15 カ国がチャット・コントロール提案を支持するようになり、以前の反対姿勢が覆った。ドイツは依然として態度を保留しており、 10 月の採決において同国の立場が極めて重要となる。以前は反対していたフランスが賛成に転じ、計画にとっての転換点となった。

2025/8/6

fightchatcontrol.eu 開設
本ウェブサイトは、チャット・コントロール提案に関する情報と最新情報を提供するために開設された。本提案がもたらす影響についての認識を高め、これに反対する世論を喚起することを目的としている。

2026/3/26

「チャット・コントロール 1.0 」の延長案が否決!
重要な修正案 34 （未知の写真やテキストの自動評価を拒否する内容）が 1 票差で可決され、これにより「チャット・コントロール 1.0 」の延長案が圧倒的多数で否決される道が開かれた。

Fight
Chat
Control

反対の理由とは

01 あなたにも影響が及ぶ

あなたが送信するすべての写真、メッセージ、ファイルが、あなたの同意や疑いもなく、自動的にスキャンされる可能性がある。これは犯罪者を捕まえるためではない。欧州連合（ EU ）の 4 億 5000 万人の市民全員に課される大規模監視だ。

02 大規模監視

すべてのプライベートメッセージ、写真、ファイルが自動的にスキャンされる。疑いの有無は問われず、例外もない。

03 基本的権利

EU 憲章第 7 条および第 8 条で保障されているプライバシーとデータ保護に関する基本的権利を損なう。これらは欧州の民主的価値観の中核をなす権利とされている。

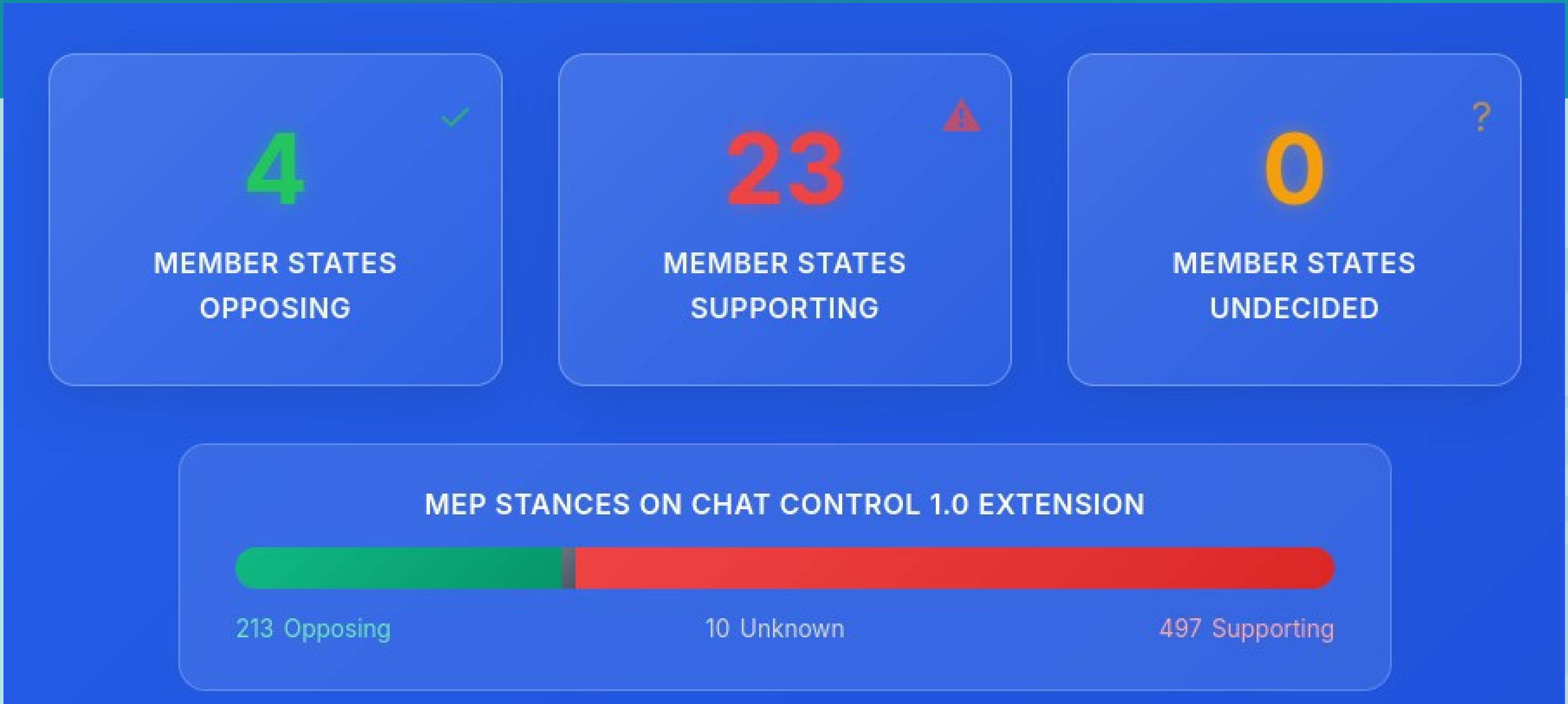
04 誤検知

自動スキャナーは、休暇中の写真や内輪の冗談といった無害なコンテンツを違法なものとして誤って識別することが常であり、人々を冤罪や捜査の妨害というリスクにさらしている。

https://fightchatcontrol.eu/

EU のチャット・コントロール

反対している国は 4 カ国、支持する国、議員が多数を占めている . . .



まとめ

日本の国家情報会議 / 局の設置は、世界各国で展開されている網羅的な監視体制構築のなかで理解する必要がある。

- いずれの国でも、最大限可能な限り人々の通信情報を収集しようとしている。
- 通信情報の収集・解析にとって暗号化が最大の障害になっていることから、暗号化の規制、弱体化が図られている。
- 暗号化を維持しつつ、警察や政府機関にだけ暗号解読が可能な「裏口（バックドア）」を設けるために通信事業者などの協力を強制している。
- 移民排斥、中東での戦争や地域の軍事的な緊張などを背景に、国家安全保障を優先させプライバシーの権利や人権を後退させる傾向がみられる。

まとめ
闘いの重要ないくつかの課題
- 子どもの人権、テロ・武力侵略からの防衛、犯罪対策など、世論の合意を得やすいトピックを利用して、私達のコミュニケーションの権利を後退させる政府の作戦に対して、私達の弱点がどこにあるのかを見定めること。
- 秘匿性の高いアプリ＝犯罪者の道具といったキャンペーンに対して、むしろ秘匿性の高いアプリを日常のツールとすること。
- 政府の網羅的な監視は、私達のスマホやパソコンなど身近な必需品を介して行なわれることを自覚した、個人をベースにした技術的な対策の有効性を確認すること。
- その上で法制度への反対運動で世論を説得すること。

おわり！
:)